SonicWALL TZ 170 SP FAQ

OVERVIEW

How is the TZ 170 SP different from the TELE3 SP?
The TZ 170 SP is the next-generation replacement for the original SonicWALL TELE3 SP -- one of the industry's first Firewall/VPN devices with an internal analog modem for failover/failback capability. The new TZ 170 SP is significantly faster, contains an internal 10/100Mbps switch for its LAN ports, has an optional interface for future growth, and runs SonicWALL's award-winning SonicOS operating system, which allows it to perform many more tasks than the original TELE3 SP. With the release of SonicOS 2.6 Enhanced for TZ 170 SP, customers will be able to back up two dedicated WAN interfaces with the analog modem's failover/failback capability, offering a levels of uptime and redundancy not found in most competitors' devices.

HARDWARE/SOFTWARE FEATURES

Can I run SonicOS Enhanced on the TZ 170 SP?
Yes.

What does the 'SonicOS 2.6 Enhanced for TZ 170 SP' upgrade cost?
The upgrade retails for US$500. This price applies to the 10-node, 25-node, and Unrestricted-node models of the TZ 170 SP.

Can I import a prefs file from a TELE3 SP into a TZ 170 SP?
You can, although it will import and report errors, and some settings will not be transferred since the hardware and prefs storing mechanisms are different in the two models. If you are replacing a TELE3 SP with a TZ 170 SP, it's recommended that you recreate the TELE3 SP's settings on the TZ 170 SP to avoid any potential issues.

How do I upgrade a TZ 170 SP from SonicOS Standard to SonicOS Enhanced?
When you purchase the upgrade, you will be provided with a new firmware image to install onto the TZ 170 SP; the new firmware is installed in the standard SonicWALL method of software upgrade (i.e. using the web management GUI and a modern web browser). Please note that since the preferences files for Standard and Enhanced are different, all settings will be erased when upgrading a TZ 170 SP from Standard to Enhanced. Because of this, you will need to note all the settings currently on the device, and re-enter them once the TZ 170 SP reboots running Enhanced.
For a more complete discussion of this topic, please see the SonicWALL whitepaper 'Upgrading SonicOS Standard to SonicOS Enhanced', located at
http://www.sonicwall.com/services/pdfs/SonicOS_Standard_to_Enhanced_Upgrade.pdf

Can I downgrade a TZ 170 SP running SonicOS Enhanced to SonicOS Standard?
Yes, but your SonicOS Enhanced preferences are not convertible to SonicOS Standard (the advanced objects in SonicOS Enhanced cannot be mapped onto the SonicOS Standard preference structure), so all settings will be lost when the TZ 170 SP reboots with SonicOS 2.x Standard.

Is there an external preferences conversion utility for older SonicWALL firmware (6.x) to SonicOS Standard and Enhanced?
No.

Is there an external preferences conversion utility for SonicOS Standard to SonicOS Enhanced?
Yes, but it only converts VPN settings, and will not convert any of the other settings. This utility is available from SonicWALL's tech support organization.

Can I manage my TZ 170 SP remotely using SonicWALL Global Management System (GMS)?
Yes, the TZ 170 SP can be centrally managed using SonicWALL's award-winning Global Management System version 2.8 or newer.

Can I use my TZ 170 SP with ViewPoint?
Yes, with Viewpoint 2.8 and newer.

What is the minimum firmware for the TZ 170 SP?
The minimum level of firmware the TZ 170 SP can run is SonicOS 2.6 Standard. The TZ 170 SP does not support older SonicOS releases, or any of the older "6.x"-series firmware releases.

How do I get firmware for the TZ 170 SP?
SonicOS 2.6 Standard is available to customers for 90 days after they have registered their devices on the https://www.mysonicwall.com customer portal, and for customers who have valid support contracts. After 90 days, customers must purchase a support contract in order to continue to receive firmware updates and new versions. When SonicOS Enhanced for TZ 170 SP is released, it will also be available for download at mysonicwall.com for those that have purchased the SonicOS Enhanced Upgrade.

What is the difference between signed and non-signed firmware?
The TZ 170 SP requires signed firmware images, unlike other SonicWALL Firewall/VPN devices. This is a new security mechanism added to the firmware to prevent tampering, and ensures that the image is both valid and originates from SonicWALL. Because of this, the TZ 170 SP will not accept non-signed firmware images. All signed images end with a '.sig' extension.

What exactly is a "security zone"?
A security zone is simply a logical grouping of one or more interfaces or subinterfaces, and is intended to make creating security policies a much simpler task. With SonicOS Enhanced, interfaces do not have the same importance in terms of how the security policy functions as they did in previous versions of firmware. Please refer to the whitepaper 'Security Zones in SonicOS 2.x Enhanced' for a full discussion on this topic.

What is the "Multicast" zone?
This is a default system zone introduced in SonicOS 2.5 Enhanced, and cannot be deleted or edited. You do not need to do anything with the Multicast zone's firewall access rules in order to get multicast to work; the system automatically writes all necessary rules. Please note that the Multicast zone will not show up on the 'Firewall > Access Rules' page unless you activate Multicast on the firewall and set one or more interfaces to participate in Multicast.

What are zone 'Security Types' and what do they mean?
In SonicOS 2.5 Enhanced and newer, there are three zone types defined: 'Trusted', 'Public', and 'Wireless'. Any zone set to 'Trusted' will automatically have security policy written to allow any systems in that zone to access systems in all other zones set to 'Trusted', and vice versa. Any zone set to 'Public' will automatically have security policy written to allow any systems in that zone to access systems in all other zones set to 'Public', but will have security policy written to deny all systems in that zone to access systems in any zone set to 'Trusted' or 'Public'. Any zone set to 'Wireless' will gain two new tabs: a 'Wireless' tab that allows you to enforce WiFiSec for all users in that zone, and a 'Guest Services' tab that allows you to enforce wireless guest services for all users in that zone. It will also write security policy to allow all systems in that zone to access system in all other zones set to 'Public', but will but will have security policy written to deny all systems in that zone to access systems in any zone set to 'Trusted' or 'Wireless'.

What does 'Allow Interface Trust' mean for a zone?
When this box is checked, all interfaces added to the zone will automatically have security policy written to allow all systems connected to each interface to talk to each other – if checked, you will see these policies show up in the firewall access rules policy intersection for that zone (for example: 'LAN > LAN'). These polices can be adjusted as needed, or deleted completely.

I created some zones, but they do not show up in the rules matrix – why?
Zones will not display in the access rules matrix unless an interface has been explicitly bound to the zone. Once an interface has been added to a zone, it will then show up in the matrix, and you can then write rules to/from this zone.

How many SonicPoints can I add to a TZ 170 SP?
You can add up to two SonicPoints to the OPT interface, once the OPT interface is added to a Wireless zone. Please note that the TZ 170 SP must be running SonicOS 2.6 Enhanced or newer to support SonicPoints.

Can I put SonicPoints in the LAN or WAN zone?
No, you cannot. In order for SonicPoints to be acquired, provisioned, and controlled by the TZ 170 SP, they must be placed into a Wireless zone. The WAN and LAN zones also do not have the WiFiSec and WGS enforcement tabs, as the Wireless zones do. While a SonicPoint can be configured to run in standalone mode and could conceivably be hand-programmed and attached to the LAN zone, you'd lose WiFiSec and WGS capabilities for the wireless users associating with that SonicPoint.

Can I connect a third-party wireless access point to the TZ 170 SP?
Yes and no – it's not possible to connect a non-SonicWALL access point to a Wireless zone, as the TZ 170 SP will not communicate with third-party access points, and will block all wireless traffic attempting to connect through it from that access point. However, it is possible to hook a third-party access point to any zone not marked as a wireless zone, but you will not be able to enforce WiFiSec or WGS for any wireless user connecting through that access point.

What is 'Consistent NAT'?
This is a new feature in SonicOS 2.5 Enhanced and newer. The control for this feature, which is located on the 'Firewall > VoIP' page, should be left unchecked by default. The Consistent NAT option modifies the SonicWALL's standard NAT behavior when handling outbound UDP traffic in order to provide higher levels of compatibility with a small handful of certain peer-to-peer applications such as some online games and Apple's 'iChat' application. Consistent NAT uses an MD5 hashing method to consistently assign the same remapped (i.e. Network Address Translated) public IP address and public UDP port pair to each internal private IP address and private UDP port pair. For example:

Private (LAN) IP: 192.168.168.10 --> Consistent Remapped Public (WAN) IP Address: 64.41.140.167
Private (LAN) UDP Port: 50650 --> Consistent Remapped Public (WAN) UDP Port: 40004

Private (LAN) IP: 192.168.168.10 --> Consistent Remapped Public (WAN) IP Address: 64.41.140.167
Private (LAN) UDP Port: 50655 --> Consistent Remapped Public (WAN) UDP Port: 40745

Private (LAN) IP: 192.168.168.20 --> Consistent Remapped Public (WAN) IP Address: 64.41.140.167
Private (LAN) UDP Port: 50650 --> Consistent Remapped Public (WAN) UDP Port: 54621

Private (LAN) IP: 192.168.168.10 --> Consistent Remapped Public (WAN) IP Address: 64.41.140.167
Private (LAN) UDP Port: 50650 --> Consistent Remapped Public (WAN) UDP Port: 49724

With Consistent NAT, all subsequent requests from either host 192.168.168.10 or 192.168.168.20 using the same Private UDP ports as illustrated above would result in the use of the same, predictable remapped Private UDP ports. Without Consistent NAT, the remapped port would change with every subsequent request, providing no consistency, and no predictability. Most UDP based applications are perfectly compatible with the latter, and do not require Consistent NAT.

There is a slight decrease to overall security as a result of the increased predictability of the traffic resulting from the consistent port remapping of Consistent NAT. The potential for exploitation is minimal; nonetheless, unless Consistent NAT is strictly required to support a certain application, it is recommended that it be left at its default setting of "disabled."

What is FIPS Mode?
FIPS, which is short for Federal Information Processing Standards, is a new feature found in SonicOS 2.5 Enhanced and newer. Enabling the FIPS Mode checkbox on the 'System > Settings' page automatically sets all necessary internal settings for a TZ 170 SP running SonicOS 2.6 Enhanced to be FIPS 140-2 compliant. Enabling FIPS mode will not change any functionality of the device, nor will it change the way the management GUI operates. Please note that since FIPS mode forces the device to use a stronger PRNG algorithm for key generation, VPN performance may be marginally affected. FIPS Mode is not supported in SonicOS Standard or any earlier version of SonicWALL firmware.

Is the TZ 170 SP ICSA-Certified?
SonicWALL has submitted the TZ 170 SP for ICSA 1.1 IPSec and ICSA 4.0 Firewall certification and is currently awaiting approval (ETA Fall 2004).

Does the TZ 170 SP support protocols other than IP?
No. The TZ 170 can only process IP traffic and cannot process IPX/SPX, NetBEUI, AppleTalk, DECNet, LAT, or SNA traffic natively. SonicOS 2.5 Enhanced and newer support GRE and Multicast. If the TZ 170 is running an earlier version of SonicOS Enhanced, or is running SonicOS Standard, in order for the TZ 170 to process such traffic it must first be encapsulated into IP packets by another device before it reaches the TZ 170's interfaces. PPTP is supported as a pass-through protocol if a specific rule is written for it.

Which routing protocols does the TZ 170 SP support?
Support for routing protocols is limited in SonicOS 2.6 – at present, the device is only capable of using RIPv1 and RIPv2 to advertise networks, for security reasons. RIP advertisements may be enabled and configured on any interface (previously it could only be enabled on the LAN and DMZ). Support for default route advertisement has been added. For each interface, the user may configure RIP to:

- always advertise the default route.
- never advertise the default route.
- conditionally advertise the default route depending on the viability of the WAN connection (non-WAN interfaces only). This taps into the wan-failover logic to determine the viability of our WAN connection(s).

The user now has the choice of enabling or disabling advertisement of remote VPN networks that are accessible via the interface for which RIP is being configured. Remote VPN networks will only be advertised when the remote address object is of the type "Network". "Range" and "Host" networks cannot be advertised. When advertisement of static routes is enabled, RIP will advertise all accessible routes, regardless of the route's egress interface. Previously, only routes that egressed out of the WAN interface were advertised. Intra-zone route advertisement (for devices running SonicOS Enhanced) will be consistent with the configuration of intra-zone communication on the 'Network >Zones' page. Dynamic routing support will be expanded in future releases of firmware.

Does the TZ 170 SP have a console-port?
Yes, it has a single RJ-45 console port. The TZ 170 SP Unrestricted-Node model ships with a RJ-45 to DB-9 serial cable to allow you to attach a workstation to the console port. In addition, the SonicOS Enhanced upgrade for TZ 170 SP includes a RJ-45 to DB-9 serial cable. The settings for the console port are 9600 bits per second, 8 data bits, No parity, 1stop bit, and no flow control. These settings cannot be modified at present. With SonicOS 2.6 Enhanced, the CLI attached to the console port is much more functional than in previous versions of firmware. The CLI's capability will be greatly expanded over the next six months.

I lost the RJ-45 to DB-9 serial cable – where can I get a new one?
You will need to contact SonicWALL tech support in order to obtain a replacement serial cable. Alternately, you can make one, using the pinouts listed below:

DB-9 Side	RJ-45 Side
1	2
2	5
3	6
4	3
5	4
6	not used
7	8
8	7
9	1

Can I operate my TZ 170 SP with the cover removed?
NO! Operating the TZ 170 SP with the cover removed can cause permanent damage to the processor and motherboard, and void the warranty. Do not power up your TZ 170 SP with the cover removed.

What are the interfaces on the TZ 170 SP?
- LAN - 5 port 10/100 Mbps switch
- Opt. Zone – 1 port 10/100 Mbps port (NOTE: disabled in SonicOS 2.6 Standard)
- WAN – 1 port 10/100 Mbps
- MODEM – 56Kbps V.92 analog modem

Are all of the fixed Ethernet interfaces on the TZ 170 SP AutoMDIX-capable?
Yes, all Ethernet interfaces are capable of automatically sensing polarity and adjusting to the cable type attached to the interfaces (i.e. straight-through or crossover). Users are now free to attach either type of cable to the interfaces when connecting the TZ 170 SP. Please note that if auto-negotiation of speed and duplex is disabled on a port, it will also disable AutoMDIX.

Can I individually set the speed and duplex of the LAN switch's 5 ports?
No, this is not possible. The speed and duplex configuration settings for the LAN interface apply to all five ports.

Can I hook a hub or switch up to the TZ 170 SP's switch ports?
Yes, you can cascade hubs/switches off any interfaces on the TZ 170 SP.

Can I assign the LAN switch ports to different zones?
SonicOS 2.x Standard does not employ the Zone paradigm; interfaces will serve as the top level of the configuration hierarchy. Upgrading to SonicOS Enhanced will offer up to three Zones (LAN, WAN, and a configurable Zone) but the switch ports will be addressed as a single logical interface statically assigned to the LAN Zone.

What are the physical specs for the TZ 170 SP?
- Dimensions: 9.07 x 6.80 x 1.63 inches (23.03 x 17.27 x 4.14 cm)
- Weight: 1.40 LBS
- Power Supply: 5V, 2.4A; 12W
- Input Power: 100-240VAC, 50-60Hz, 600mA
- Max Power: 8.5W
- Environment: Temperature: 40-105 °F, 5-40 °C, Humidity: 10-90% non-condensing
- Regulatory: EMC: FCC Class B, ICES Class B, CE, C-Tick, VCCI, BSMI, MIC
- Safety: UL, cUL, TUV/GS, CB, NOM
- MTBF: *TBD*
- Total Heat Dissipation: 29BTU
- Modem: V.92 Analog Modem

How much memory is on the TZ 170 SP?
The TZ 170 SP contains 8MB of onboard, non-upgradeable flash, and 64MB of onboard, non-upgradeable RAM.

What kind of processor does the TZ 170 SP use?
The TZ 170 SP uses a multifunction MIPS RISC-based security processor that handles all processor-based I/O functions, as well as all crypto functions (3DES, AES, MD5/SHA-1, DH, and ESP) directly in hardware. This significantly speeds all crypto functions for VPN traffic.

What does the 'Opt. zone' interface do?
If the TZ 170 SP is running SonicOS 2.6 Standard, the 'Opt. Zone' interface is disabled and cannot be used. A future release of SonicOS Enhanced for the TZ 170 SP will enable this interface and allow it to be used as an additional internal interface, as a DMZ interface, or as a secondary WAN interface.

Can I run the TZ 170 SP in transparent mode?
No, it's not possible to use transparent mode when running SonicOS Standard.

Can I change the default IP address of the LAN interface?
Yes. The devices ship with 192.168.168.168/24 as the default IP address, for the LAN interface but can be changed to any value. Please note that the new value will take effect as soon as the 'OK' button is clicked, so you will need to change the IP address of your management station to match the new IP subnet of the LAN interface, and then log back into the device to continue setup.

Can I assign multiple IP addresses to the LAN interface?
Yes, as long as they are from unique subnets.

How long does it take for the TZ 170 SP to start up?
The average startup time from power-on to operation is approximately one minute. The device performs a number of hardware and software diagnostic check routines upon warm and cold boots to ensure the device, modem, and firmware are fully operational.

I activated SonicWALL Content Filtering System (CFS) Premium, enabled all the categories, and none of the systems behind the SonicWALL can access any site on the public Internet – why?
SonicWALL CFS Premium Editions contain a large number of new categories that, if activated, will block systems from accessing sites that may seem innocuous, such as search engine portals, news media sites, and computer manufacturers' Web sites. There is also a final category called 'Not Rated' that, if checked, will block access to any site that is not in the CFS Premium database. Because of this, you will need to carefully choose the appropriate categories for the CFS Premium policy applied to the SonicWALL's zones.

I have AV enabled on an interface, but I can't seem to install the client on my system – why?
The AV installation is done via browser and relies on a pop-up window to install properly. If you are not able to install the SonicWALL AV Client on a system, check to see if the system's web browser is actively blocking pop-ups, or that it does not have a third-party program (such as 'Pop-Up Stopper') that is blocking the AV installation screen. In order to install the SonicWALL AV Client, you must allow pop-ups during this process.

Can I assign multiple public IP subnets to a WAN interface?
It is not currently possible to assign more than a single IP address to a primary or secondary WAN interface, but the device is capable of answering on behalf of a 1-2-1 NAT policy set up for a network resource. This is useful in environments where an ISP has assigned a customer multiple dissimilar public IP subnet blocks, and the customer wishes to use IP's from these dissimilar blocks to provide access to internal network resources. What is required is for the ISP's upstream routing be capable of routing these subnets to the fixed IP address of the primary or secondary WAN interfaces of the SonicWALL.

Is there an easy way to erase the config file on the TZ 170 SP?
This is done from the 'System > Settings' menu by booting the box with the 'Current Firmware with Factory Default' settings button. All stored settings (including username, password, and LAN IP address) will be discarded and the device will reboot with factory settings (username: admin, password: password, LAN IP Address: 192.168.168.168).

Is there an easy way to erase the firmware on the TZ 170 SP?
Simply load a new version and boot that one instead – the previous one will be erased and replaced with the new version. If the process fails, the device will boot into the SafeMode menu.

Is User-Level Authentication (ULA) supported in SonicOS 2.6 Standard?
Yes – there's a check box on the 'Users > Settings' page that, when checked, will force all systems on the LAN and OPT interface to log into the TZ 170 SP and authenticate with a username and password before any traffic is allowed to pass across the device. ULA is also supported in SonicOS 2.6 Enhanced, but is configured in a different manner (instead of an all-or-nothing mechanism, ULA is enforced on a fully granular, per-rule basis between security zones).

What is SafeMode?
SafeMode is a feature of the SonicOS Standard and Enhanced firmware that allows firewall administrators to switch between firmware builds and revert to known-good versions in case a new firmware image turns out to cause issues. In cases of firmware corruption, the device will boot into a special GUI mode that allows the administrator to choose which version to boot, and also allows the administrator to run hardware diagnostics, view the bootlog, or export the bootlog to a file.

How do I access the SafeMode menu?
In emergency situations, you can access the SafeMode menu by holding in the Reset button on the back of the TZ 170 SP (it's the small pinhole button located to the left of the Console port) for 12-14 seconds until the 'Test' light begins flashing yellow. When the SonicWALL is booted into the SafeMode menu, assign a workstation a temporary IP address of '192.168.168.200' and attach it to a LAN interface on the TZ 170 SP. Then, using a modern web browser (Microsoft IE6.x, Mozilla 1.4+), access the special SafeMode GUI using the device's default IP address of '192.168.168.168'. You will be able to boot the device using a previously saved image, or you can upload a new version of firmware with the 'Upload New Firmware' button.

Is there still a 'diag.html' page?
Yes. This page is kept to store configuration settings that are rarely used, and for extremely specific environments. Do not modify values on this page unless SonicWALL requests you do so.

VPN

What is the "VPN" zone?
The VPN zone is a special type of zone in SonicOS Enhanced, used to enforce security policy to/from all VPN connections, including GroupVPN connections. For example, if you had a single site-to-site VPN tunnel to a remote office, when you created the tunnel, the firewall automatically created default 'allow all' firewall rules for the networks you specified when creating the tunnel. If you wished to add more granular control over the traffic flowing to/from that remote site, you can go into the intersection of the internal zones and the VPN zone and adjust the rules as needed. To override firewall rules going to the remote site, you'd adjust the policy for 'LAN > VPN', and to override rules coming from the remote site, you'd adjust the policy for 'VPN > LAN'.

Can I set up VPN tunnels to older SonicWALL devices?
Yes – all versions of SonicOS are backwards compatible with all previous VPN-capable versions of SonicWALL firmware.

Can I set up site-to-site VPN tunnels from the TZ 170 SP to third-party VPN devices?
Yes, as long as the other device supports manual IPSec or IKE IPSec. This would include all other IPSec-capable SonicWALL models, and devices from other manufacturers.

How many remote access VPN sessions are supported by the TZ 170 SP?
The TZ 170 SP does not ship with any Global VPN Client licenses preinstalled, and must be upgraded with SonicWALL Global VPN Client licenses to accept incoming connections. It can support up to 50 concurrent remote access VPN sessions, when properly licensed. Also note that the 25-node and Unrestriced-node license upgrades also include 1 Global VPN Client license. The term "remote access VPN session" refers to an IPSec connection to a unique remote SonicWALL Global VPN client.

How many site-to-site VPN policies are supported by the TZ 170 SP?
The TZ 170 SP supports 10 site-to-site VPN sessions. Please note that while the license will limit connections to the number of unique remote peers, it does not limit the number of destination networks (phase two SA's) that can be negotiated for each remote peer (that number is only limited by the amount of free memory on the device). The term "VPN policy" refers to an IPSec connection to a unique remote site-to-site VPN peer, such as another SonicWALL device, or an IPSec-capable 3rd party device.

Can I use other third-party VPN clients to connect to the TZ 170 SP?
SonicWALL officially supports IPSec VPN connections to the TZ 170 SP with the older SonicWALL VPN Client (versions 5.1.3 & 8.0) for Windows-based systems, the SonicWALL Global VPN Client (version 1.x and 2.x) for Windows-based systems, the Equinux VPN Tracker (version 1.0.2) for Apple OSX 10.2-based systems, and the Funk AdmitOne VPN Client (version 2.0) for PocketPC 2002-based systems. It may be possible to make a Manual IPSec or IKE IPSec connection with other third-party clients, but SonicWALL does not endorse or support their use. If the PDA is running Pocket PC 2003, you can use the built-in L2TP client to connect to the TZ 170 SP's L2TP server; however, this feature is only supported if the TZ 170 SP is running SonicOS 2.6 Standard or newer.

My GroupVPN policy is set for AES, and some of my Global VPN Clients cannot connect – why?
AES support is only in Global VPN Client version 2.0 and newer; version 1.0 does not support it. If you are mixing 1.x and 2.x clients, you will need to specify 3DES as the encryption method for phase 1 and phase 2.

Will VPN's work across the analog modem connections?
Yes, in fact one of the primary uses of the TELE3 SP and the new TZ 170 SP is to provide a secondary failover/failback path for VPN traffic when the primary WAN interface has failed. Since most ISP POPs assign dynamic IP address information to connecting systems, it will be necessary to configure the VPN tunnels to use Aggressive Mode and to use SonicWALL Identifiers as the IKE identities on both sides. It is also possible to disable VPN traffic from traversing the analog modem when it is active, on a per-profile basis. This feature is used mainly when the TZ 170 SP is dialing into a company-owned RAS server, where it would not be appropriate for the device to attempt to re-establish its VPN tunnels, since dialing into the RAS servers may be providing direct connectivity to the resources that the VPN tunnels had been created to reach.

MODEM

What type of modem is in the TZ 170 SP?
It's a 56K V.92 modem, and can be configured to connect at auto, 2400, 4800, 9600, 14400, 19200, 38400, and 57600 speeds, on a per-profile basis.

Can I dial into the TZ 170 SP?
No, this feature is not currently supported in any version of SonicOS for the TZ 170 SP, although SonicWALL is investigating it for a future release.

Can the TZ 170 SP do dial-back?
No, this feature is not currently supported in any version of SonicOS for the TZ 170 SP, although SonicWALL is investigating it for a future release.

What is a modem profile?
A modem profile contains all the ISP POP-related settings required for the TZ 170 SP to dial out, authenticate, and connect to the public Internet. In each profile, you can specify up to two separate phone numbers, the username/password, a chat script, and whether the SP will receive its new IP address information dynamically or statically. You can also specify that the TZ 170 SP dial immediately upon primary WAN failure, or dial only on data, or manual dial (i.e. user must log into TZ 170 SP and click on 'Connect' button to dial out), as well as specify maximum connect times if needed. The TZ 170 SP has a new scheduling feature for the analog modem that allows you to limit the times it can be active, on a weekly basis.

How many profiles can you have on the TZ 170 SP?
You can create ten profile entries, but you can only specify two of them as active – one as the primary profile, and one as the alternate profile. If the phone numbers in the primary profile do not work, then the TZ 170 SP will attempt to use the alternate profile to connect. Profiles may contain login information for the same ISP but using different access phone numbers, or each profile can be configured to connect to different ISPs. In the latter case, you would need to purchase dial-up accounts with more than one ISP.

Can I specify my own AT commands?
Yes, this is done in the 'Modem > Settings' section of the TZ 170 SP's management GUI, or you can use the country drop-down provided to initialize the modem for the specified country.

How do I set up the TZ 170 SP to do modem failover?
It's simple – create a dialup profile, set the modem's initialization settings, set the dialup profile you just created as the 'Primary Profile', and then enable 'WAN Failover'. When enabling 'WAN Failover', you may optionally configure it for 'Preempt Mode', which will cause the TZ 170 SP to disconnect the analog modem once the primary WAN resource has returned to service.

What is Probing?
The TZ 170 SP has the ability to perform a physical check, as well as a logical check, of the primary WAN and the analog modem. By default, the analog modem will only become active if the primary WAN interface suffers a physical failure (i.e. is electrically disconnected). However, in environments where uptime is critical, it may be necessary to perform additional logical checks of upstream targets to ensure that the path is indeed valid. Enabling probing for the analog modem's failover/failback capabilities allows the TZ 170 SP to probe an upstream IP address via ICMP or user-definable TCP port, over the Modem, over the Ethernet, or over the Modem and the Ethernet. You can also specify the probe interval, the failover trigger level, and the successful number of probes required to reactivate the primary WAN interface.

Quick Speeds/Feeds Chart for TZ 170 SP w/SonicOS 2.6 Standard

Feature	*Number*
Firewall Performance	90 Mbps
VPN Performance	30 Mbps
Concurrent firewall connections	6,144
Max Concurrent Site-to-site VPN connections	10
Max Concurrent Client VPN connections	50
Number of Site-to-site VPN licenses device ships with	10
Number of Client VPN licenses device ships with	0
Can upgrade concurrent Site-to-site VPN connections?	NO
Can upgrade concurrent Client VPN licenses?	YES
Can upgrade node count licenses?	YES
Max NAT Policies/1-2-1 NAT Entries	512
Max Static IP Routes	128
Max Firewall polices	100
Max DHCP Leases (global)	1,024
Max DHCP Scopes	2
Max Internal User Accts	100
Max Internal User Groups	N/A
Max Guest User Accts	100
Max Address Objects	N/A
Max Address Object Groups	N/A
Max Service Objects	N/A
Max Service Object Groups	N/A
Max Schedule Objects	N/A
Max SonicPoints per interface	2 on OPT port (requires SonicOS Enhanced)
Max SonicPoints supported on device	2 on OPT port (requires SonicOS Enhanced)

Document Created: 06/14/2004
Document Updated: 08/10/2005
Document Version: 1.4
Document Maintained By: Dave Parry